دليل الأمان الرقمي



مقدمة

بالرغم من عدم امتلاك غالبية المصريين لأدوات التكنولوجيا، إلا أن عددًا غير قليل يستخدم الحواسيب والهواتف الذكية يوميًا، على المستويات العملية والشخصية. ومؤخرًا أصبحت هوياتنا الرقمية جزءً مهمًا جدًا من هوياتنا الواقعية. نستخدم يوميًا أدوات رقمية مثل البريد الإلكتروني ومنصات التواصل الإجتماعي، وبرامج التواصل اللحظي، ووسائل مشاركة الملفات وحتى برمجيات شركات عالمية لنقل الركاب، كل هذه البرمجيات والمنصات والأدوات تعرف الكثير عنا؛ معلومات عن مراسلاتنا وأقرب الأصدقاء لنا، والأماكن التي نتردد عليها، علاوة على صور ومواد مصورة وملفات وغيرها الكثير. لذا فمن المهم لنا أن نعرف المخاطر التي تتعرض لها هوياتنا و بياناتنا الرقمية، لتكون لدينا القدرة والمعلومات الكافية لحماية هويتنا وبياناتنا. فبقدر ما وفرت لنا التكنولوجيا الحديثة أدوات وطرق لتخزين وتداول المعلومات بإمكانات غير مسبوقة، ففي نفس الوقت و بذات القدر، عرضت هذه البيانات لمخاطر غير مسبوقة، ووضعتنا أمام تحديات أكبر.

لماذا أصدرنا هذا الدليل؟

تعتبر متون الأمان الرقمي أحد أهم الملفات التي تعمل عليها من خلال التدريب وتقديم الاستشارات التقنية للمؤسسات والشركات والأفراد، لذلك رأينا –من خلال الاحتكاك مع فئات عديدة أثناء عملنا في هذا المجال– أنه حان الوقت لإعداد دليل يلقي الضوء على بعض العادات الرقمية التي اعتاد الجميع فعلها ظنًا أنها تسهل استخدامهم الرقمي أو أنها أكثر أمانًا، حيث وجدنا أن معظم حالات الانتهاك الرقمي التي تعرضنا لها مع مؤسسات أو أفراد معظمها يندرج بشكل واضح تحت مسمى "العادات الرقمية الخاطئة"، والتي بالتأكيد تسهل على المستهدف الوصول لهدفه أيًا كان هو، سواء اختراق حسابات رقمية أو الاستيلاء على بيانات لتحقيق أغراض مختلفة. نهتم في هذا الدليل بالأساس بتوعية مستخدمي التكنولوجيا بتلك العادات التي تعرضهم والآخرين للخطر، دون وعي منهم بذلك. وجدنا أيضًا أنه من الضروري إعطاء نصائح وترشيحات لبرمجيات وأدوات بديلة وآمنة، محاولة منا لمساعدة كل من يطلع على هذا الدليل، ليس فقط في إدراك المخاطر التي قد يتعرض لها ولكن أيضًا طرح حلول للوصول للحد المتوسط من الأمان الرقمي.

المنهجية المتبعة في إعداد هذا الدليل

اعتمد فريق عمل هذا الدليل على قصص واقعية، وذلك بعد عقد ورشة لجمع قصص عن الانتهاكات الرقمية بمساعدة بصي، إضافة إلى مواقف تعرض لها الفريق التقني في متون أثناء تقديم خدمة العيادة التقنية على مدار عامين من تقديم الدعم اللازم لحالات تعرضت لانتهاكات رقمية. رأى الفريق أنه من الأفضل توضيح المخاطر الرقمية من خلال وقائع حقيقية، لأنها بشكل كبير تعبر عن غالبية المخاطر التي نتعرض لها جميعًا، إما بسبب عادات تعودنا على فعلها بشكل يومي أو استخدام أدوات وبرمجيات لا يتوفر فيها عناصر الأمان لمجرد أنها أكثر شيوعًا في مجتمعاتنا. لذلك اخترنا سبع قصص واقعية، تتشابه تفاصيل الكثير منها وتتكرر فيها الأخطاء، لإبراز كيفية تلافي المخاطر الرقمية وترشيح أدوات وبرمجيات آمنة لتلاشي الوقوع في نفس المخاطر مرة ثانية. يبدأ الدليل بتوضيح كيف يعمل الإنترنت، ثم سرد لأبرز الجهات التقنية التي لها صلاحيات لمعرفة بياناتك واستكشاف هويتك الرقمية، لأغراض تجارية أو أمنية أو شخصية. وينتهي الدليل، بملحق يحتوي معلومات تقنية عن الأدوات والبرمجيات التي يرشحها فريقنا التقني، تستطيعون من خلالها معرفة أهم خصائصها ومميزاتها، وكذلك روابط موثقة توضح كيفية استخدامها وفقًا لنظام التشغيل الذي تستخدمونه.

حقنا في الخصوصية

نعتبر هذا الدليل مساهمة بسيطة في ترسيخ المادة ١٢ من الإعلان العالمي لحقوق الإنسان، وهي وثيقة تاريخية هامة في تاريخ حقوق الإنسان، صاغه ممثلون من مختلف الخلفيات القانونية والثقافية من جميع أنحاء العالم، واعتمدت الجمعية العامة للأمم المتحدة، الإعلان العالمي لحقوق الإنسان في باريس في ١٠ ديسمبر ١٩٤٨، بموجب القرار ٢١٧ أ، بوصفه أنه المعيار المشترك الذي ينبغي أن تستهدفه كافة الشعوب والأمم. وهو يحدد، و للمرة الأولى، حقوق الإنسان الأساسية التي يتعين حمايتها عالميا.

نص المادة ١٢:

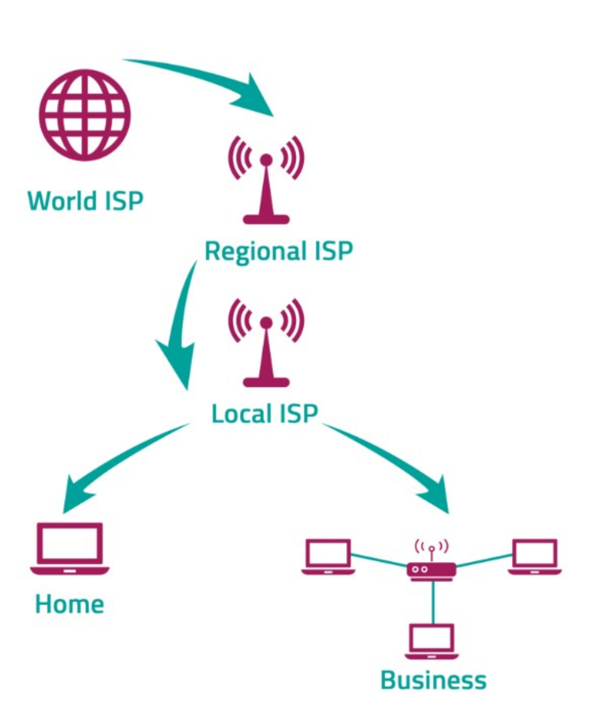
لا يجوز تعريضُ أحد لتدخُّل تعسُّفي في حياته الخاصة أو في شؤون أسرته أو مسكنه أو مراسلاته، ولا لحملات تمسُّ شرفه وسمعته. ولكلِّ شخص حقٌّ في أن يحميه القانونُ من مثل ذلك التدخُّل أو تلك الحملات.

كيف يعمل الإنترنت؟

من الضروري معرفة كيف يعمل الإنترنت لفهم أفضل للمخاطر التي تواجهنا عند استخدام التطبيقات والأدوات التقنية المذكورة في هذا الدليل. يمكننا القول أن الإنترنت ببساطة هو شبكة ضخمة تتكون من شبكات أصغر منها متصلة ببعضها، داخل تلك الشبكات تتواجد مليارات من الحواسيب والمعدات التي تتصل ببعضها البعض عن طريق بروتوكول الإنترنت (IP) لمشاركة كافة أنواع المحتوى سواء علنًا أو بوصول محدد وحصري.

عندما تكتب في متصفحك اسم الموقع الذي ترغب بالإطلاع على محتواه، يرسل المتصفح طلبًا يحتوي معلومات عديدة من بينها اسم نطاق الموقع (Domain name)، مثل Google.com، إلى خواديم مخصصة لهذا الغرض تحوّل اسم النطاق إلى عنوان بروتوكول الإنترنت الخاص بالخادوم الذي يحتوي على الموقع المقصود، ليتوجه المتصفح إليه بطلب جلب المحتوى عن طريق البروتوكول المناسب (بروتوكول نقل النص التشعبي HTTP في حالة الاطلاع على صفحة وب).

وهكذا فإن أغلب بروتوكولات الاتصال داخل الإنترنت تعتمد على علاقة الخادم\العميل (Server/client) في إدارة اتصالاتها.



ماذا يعرف عنك هؤلاء؟

مقدم خدمة الإنترنت (ISP):

عند اتصالك بالإنترنت بدون أي إجراءات تأمين إضافية فإن مقدم خدمة الإنترنت لديه إمكانية الإطلاع على هذه البيانات:

عنوانك على الإنترنت (IP) ومكانك الجغرافي.

المواقع التي تطلبها وأسماء نطاقاتها.

المحتوى الذي تصل إليه (في حالة عدم استخدام مواقع مؤمنة عن طريق بروتوكول نقل النص التشعبي الآمن HTTPS).

في حالة استخدام الإنترنت من خلال هاتف ذكي فيمكنه أيضًا معرفة نوع الجهاز، والشركة المصنعة، ومكانك في الوقت الحقيقي.

مدير الشبكة المحلية في العمل أو الفندق أو في الشبكات العامة والمفتوحة:

عنوانك على الإنترنت (IP) ومكانك الجغرافي.

المواقع التي تطلبها وأسماء نطاقاتها.

المحتوى الذي تصل إليه (في حالة عدم استخدام مواقع مؤمنة عن طريق بروتوكول نقل النص التشعبي الآمن HTTPS).

فيسبوك:

تعتبر خدمات فيسبوك من أكثر التطبيقات نهمًا للبيانات، فعندما تفتح موقع فيسبوك على متصفحك يستطيع جمع هذه المعلومات:

يتمكن الموقع من تسجيل حركات مؤشر الفأرة والمواقع الأخرى المفتوحة في نفس الوقت داخل نفس المتصفح.

مكانك الجغرافي ونوع حاسوبك ونظام التشغيل والمتصفح الذي تستخدمه.

يسجّل ويحلل بياناتك بالكامل لبناء صورة كاملة عن تفضيلاتك الشخصية وعاداتك على الإنترنت، من أجل استغلال تلك البيانات لاحقًا في توجيه الإعلانات التي لها فرص أكبر في لفت انتباهك.

عند استخدام تطبيق فيسبوك من خلال هاتف ذكي يمكن أن نلاحظ بسهولة كم صلاحيات الوصول التي يطلبها التطبيق عند تنصيبه (الكاميرا - الميكروفون - سجل الهاتف - وحدة التخزين - الحساسات الإلكترونية - الموقع الجغرافي).

القصص

القصة الأولى

"لأ دا كان موبايلك، دا لوقتي بقى بتاعي!"

كنت في حفلة عيد ميلاد، وعلى نص الحفلة حسيت بضيق فقررت أمشي بسرعة، بعد ما وصلت البيت افتكرت إني نسيت موبايلي، رجعت تاني على مكان الحفلة ودورت وما لاقيتش الموبايل، وسألت المسؤولين عن المكان قالولي : "لأ مش موجود"، رجعت البيت وأنا زعلانة جدا على ضياع الموبايل. وأنا في البيت لقيت شخص غريب بعت لي إضافة على فيسبوك، الشخص دا كان حاطط صورتي وحاطط كل حاجة عني ما عدا إسمي، وبصراحه ما عرفتش أعمل إيه فقلت أقبل الإضافة وبقى عندي في أصدقاء فيسبوك، في أصدقاء عندي قالوا لي: "خلي بالك دا مزيّف، دا بيسرق كل حاجة عنك". وفي نفس اليوم لقيت واحد بيبعت لي طلب إضافة.

وكنت قاعدة فاضية وما كانش عندي مشكلة أفتح حوار مع حد فقبلت الطلب، وفتح معايا كلام، وسط كلامه حسيت أنه يعرف عني حاجات أو عاوز يعرّفني إنه يعرف عني حاجات، ما توقعتش أني أعرفه لأني لو أعرفه شكله كان هيبقى مألوف، بس ساعتها عرفت أن فيه حاجة غلط و قعدنا نتكلم كل يوم لمدة ٣ أيام.

وفي يوم قررنا نتقابل، ولما اتقابلنا في الكافيه فضل يقول لي على حاجات كتير عني أنا ساعتها خفت الصراحة، ما عرفتش هو عرف المعلومات دي من فين.







وبعد ما طلعنا من الكافيه عرض عليا إنه يوصلني وانا ركبت معاه العربية وفي نص الطريق قال لي: "أنت مش عاوزة تعرفي أنا اعرف الحاجات دي كلها عنك من فين؟"، وفجأة فتح لي التابلوه وطلع الموبايل بتاعي، سحبته بسرعة من إيده وقلت له: ”ده موبايلي!“

قالي : لأ دا كان موبايلك، دلوقتي بقى بتاعي“

”جبته منين؟“

”جبته من شارع شاكور، ولما اشتريته كانت كل الإيميلات مفتوحة والصور بتاعتك كلها موجودة“

أنا ساعتها استغربت جدا وطلبت منه يقفل الإيميلات ويمسح كل الصور من عليه، وعدت الأيام ولقيته بيكلمني تاني عشان نتقابل أو نخرج وأنا رفضت رفض قطعي، ساعتها بدأ يهددني بالرسائل والصور اللي كانت على موبايلي.

لحماية خصوصيتك على هاتفك الذكي ننصح باتباع الخطوات دي:

اختيار كلمة سر قوية وغير متوقعة لهاتفك.

تفعيل خاصية تتبع الهاتف فى حالة سرقته أو ضياعه.

تفعيل خاصية التعمية.

لا تقبل إضافة أشخاص لا تعرفهم.

إذا كنت تشتري هاتفًا جديدًا:

يجب التأكد عند شراء هاتف يعمل بنظام أندرويد من دعم إصدار نظام التشغيل لخاصية التعمية الكاملة لوحدة التخزين، إذ يوجد بالأسواق عدة إصدارات لا تدعم التعمية (بعض هواتف شركة هواوي على سبيل المثال).

تفعيل خاصية التعمية الكاملة لوحدة التخزين واختيار كلمة سر قوية لفتح وقفل الهاتف.

بالنسبة لهواتف أبل، تأتي أغلب الإصدارات الحديثة نسبيًا منها، بخاصية التعمية الكاملة لوحدة التخزين مفعلة مسبقًا دون تدخل من المستخدم.

تفعيل خاصية تتبع الهواتف في حالة الاستحواذ المادي عليه.

القصة الثانية

"طبعًا حضرتك مش لاقيه اللابتوب، وريني هتشتغلي إزاي بعد كده!"

من حوالي سنتين، كان في خلافات بيني وبين زوجي كبيرة جدًا وصلت إننا اطلقنا، في يوم اتخانقنا خناقة كبيرة جدًا بسبب أنه كان رافض أني أستمر في الشغل وعايزني أقعد في البيت لأن بيتي أولى بيا! أصريت وقتها على قراري إني مش هسيب شغلي فهددني أنه هيطلقني وهياخد ولادي وتقريبًا طردني من البيت، الخناقة كبرت بنا وقلت له إني مش هسيب بيتي ولا ولادي ولا هسيب شغلي، وسبته ودخلت أوضة النوم أنا وولادي وقفلت عليا ونمت.

الصبح كلمت ماما تيجي تقعد بالأولاد لحد ما أرجع من الشغل، ويادوب فطرت وجهزت عشان أنزل أول ما ماما توصل لأني كنت متأخرة، وأنا بلم حاجتي مالقيتش اللابتوب بتاعي! دورت عليه في كل مكان في البيت وبرضو ما لقيتهوش! توقعت أنه يكون أخده كنوع من لوي الدراع عشان فاكر أنه هيعطلي شغلي لأنه عارف كويس أن شغلي كله متخزن على اللابتوب الشخصي مش على جهاز الشغل.

أول حاجة عملتها أني كلمته، بس فضل كتير ما يردش عليّ! وبعدها بعت لي على واتساب "طبعًا حضرتك مش لاقيه اللابتوب، وريني هتشتغلي إزاي بعد كده"، طبعًا كنت في حالة غضب شديدة قررت فيها إني مستحيل أعيش مع شخص سرق حاجتي وبيلوي دراعي عشان عارف إن شغلي كله عليه، بما أني محامية فهو عارف أن في مرافعات ومذكرات كنت كتباها على جهازي وبطبعها قبل تقديمها للمحكمة مباشرةً وده طبعًا معناه أن شغل شهر و شهرين جايين هيتعطل!

رفعت قضية خلع على طول من غير أي تردد. و بعد شهور في إجراءات القضية فوجئت أنه بيبعتلي صور شخصية كانت على الجهاز وبيهددني إني لو مرجعتش عن القضية هيرفعهم على النت، قررت أتجاهل رسايله



لحد ما في يوم لقيته باعت رسايل تشويه لسمعتي لموكلين على إيميلاتهم من إيميلي الشخصي. عرفت بعدها كمان انه كان بيتتبع كل حاجة في شغلي من خلال إيميلي اللي كان بيقدر يفتحه طول ما الجهاز معاه.

لحماية جهاز اللابتوب الشخصي، ننصح باتباع الخطوات دي:

استخدام نظم تشغيل تدعم خاصية حماية البيانات.

الاحتفاظ بنسخ إحتياطية للبيانات و بالأخص الهامة منها على وحدة تخزين خارجية.

اختيار كلمات سر قوية وغير متوقعة لجهازك الشخصى.

نظام التشغيل و التعمية هما مدخلك للحفاظ على بياناتك على جهازك الشخصي:

ضروري جدًا استخدام نظام تشغيل آمن قبل كل شيء وما نكتفيش بكلمة السر لأن ممكن جدًا كسرها في أغلب أنظمة التشغيل.

مهم كمان أن نظام تشغيل يكون يدعم تعمية وحدة تخزين البيانات بشكل كامل، ودا يعتبر الضامن الوحيد لعدم الاستيلاء على البيانات في حالة الاستحواذ المادي على جهازك.

من مفيد استخدام برمجيات تانية لتعمية بيانات محددة على القرص الصلب وضروري دايمًا الاحتفاظ بنسخ احتياطية معمّاة من تلك البيانات على وحدات تخزين خارجية، مع الحرص بالتأكيد على استخدام برمجيات موثوقة وكلمات سر قوية في عملية التعمية.

الأدوات والبرمجيات المقترح استخدامها في تلك الحالة:

Veracrypt

Full disk encryption on GNU/Linux

”Bitlocker “Windows

”Filevault “MAC

القصة الثالثة

"أنت فتحت الكمبيوتر بتاعي!"

لازم ابدأ الحكاية بإعلان مهم: أنا بآخد صور عريانة لنفسي، دا جزء من أسلوب دفاعي أنا اخترعته لنفسي عشان أحب جسمي في مجتمع كل يوم فيه إعلانات عن منتجات تخسيس وجراحات تجميل بتخليني أكره شكل جسمي والسيلولايت، كنت بحاول دايما آخد صور لنفسي وأبص لها وأقول حاجات إيجابية عنها وألاقي في كل تفصيلة فيها جمال غصب عن كل معايير المجتمع المقرفة.

من سنتين كان معايا تليفون بيرفع الصور بشكل تلقائي على دروب بوكس (Dropbox) بتاعي، ودروب بوكس بتاعي باستخدمه في كل حتة؛ في الموبايل، وكمبيوتر الشغل، واللاب توب الشخصي.

وما كنتش مديّة خوانة أبدًا لأي حد في الشغل، خاصةً إني كنت شغالة في مؤسسة محترمة بتدعم الحقوق. وفي المؤسسة كان فيه شخص إداري حاول يتقرب لي بشكل جنسي ورفضت فبكل بساطة واحترام قال: ”مش عايزة، براحتك“. لكن فوجئت في يوم بأن الكمبيوتر بتاع الشغل كان مفتوح وأنا مش موجودة — وكلمة سر الكمبيوتر مش موجودة إلا مع نفس الشخص الإداري. سألته بشكل صريح: ”أنت فتحت الكمبيوتر بتاعي؟“. فقال إنه أسلوبي في الكلام مش عاجبه وإني يستحسن أحسن أسلوبي معاه وإلا هيكون له تصرف تاني، وإني لو حابّة أشتكي من أي حاجة، أقدم شكوى رسمية، بالفعل قدمت شكوى رسمية.

في اليوم دا روّحت البيت لاقيت حساب على فيسبوك باعت لي إضافة. الحساب دا باسمي وعليه جزء مقتطع من صورة من صوري العريانة مستخدمة صورة الحساب. حسيت فجأة إني مش قادرة أتنفس ولا أفكر ولا حتى أعيط.

كان إحساس بشع، والأبشع إني مش عارفة هو بيعمل دا بهدف إيه، حتى الابتزاز بيبقى لهدف: مادي، جنسي، إنما دا بيعمل أذى وبس، أذى بهدف الأذى، أو الانتقام، أو ما أعرفش إيه اللي كان في نيته.



الشكوى الرسمية ما اتحركتش ببساطة لأن الشخص دا مؤتمن على ناس كتير وعمره –حسب كلام اللي اشتكت له– ما ضايق أو اتحرش أو اتعرض لأي ست منهن، ولأني ما عنديش أي دليل على إن الشخص اللي أنا بشتكي منه عمل دا بالفعل.

بعد كتير من البلاغات الحساب دا اتقفل، والشخص –واضح– إنه ما حاولش تاني. بس المشكلة إني طول الوقت بحس إني مهددة، إن فيه حد معاه حاجة مش حقه تكون معاه ويقدر يستخدمها في أي لحظة يعوزها، من غير ما أي حد يصدقني أو يعرف يوقفه.

في حالة استخدامك لحسباتك الشخصية على أجهزة العمل، ننصحك بالخطوات دي:

- فك ربط الحسابات الإلكترونية على جهاز العمل.
- اتباع الإجراءات الوقائية لحماية الجهاز والبيانات المخزنة عليه.
- استخدام نظم تشغيل لأجهزتك تدعم خاصية حماية البيانات.
- اختيار كلمة سر قوية وغير متوقعة لجهاز العمل.
- وقف خدمة التسجيل الأوتوماتيكي لحساباتك الشخصية على جهاز العمل.
- إلغاء تصريح دروب بوكس أنه يحتفظ بالبيانات تلقائيًا.

لما نحب نشارك ملفات وبيانات خاصة عبر الإنترنت، ضروري التأكد من الآتي:

- اختيار خدمة مشاركة ملفات آمنة.
- يفضل استخدام خدمة مشاركة ملفات تستخدم خدمة التعمية من الطرف للطرف (End to end encryption)، على أن تكون خدمة جيدة السمعة.

الأدوات والبرمجيات المقترح استخدامها في تلك الحالة:

- Firefox send
- Mega.nz

القصة الرابعة

"عندكم واي فاي؟ إيه الباسورد؟"

كان آخر يوم امتحان في السنة، وزي العادة طلعنا من الجامعة عشان نستقبل أجازة الصيف الطويلة، رحنا اتغدينا وبعدها قررنا نقعد في كافيه أنا وصحابي. وعادي أول ما دخلنا سألنا لو فيه واي فاي في الكافيه، أخدنا الباسوورد ودخلنا على الشبكة زي ما بنعمل في أي مكان كل يوم.

بعد شهور من اليوم دا فوجئت بحد بيبعتلي على الواتساب صور شخصية مش موجودة في أي حته غير على فيسبوك! شتمته وقتها وعملتله بلوك. بعدها لقيت رقم تاني بيبعتلي فويس نوتس لي ولقطات شاشة لكلام بيني وبين صحابي على فيسبوك! طبعًا ساعتها جالي حالة انهيار ومبقتش عارفة اتصرف ازاي غير أني اسأله أنت عايز إيه مني؟ وجبت الحاجات دي منين؟

مردش عليا وفضلت شهر كامل في حالة خوف ورعب لحد ما في يوم لقيت رقم غريب بيكلمني رديت لقيته بيقولي "أنا سيبتك تفكري إزاي هتكافئيني إني مابعتش الصور لأبوكي". قلت له أنت عايز إيه مني؟ وجبت الحاجات دي منين؟ قالي ملكيش فيه دا شغلي هتدفعي كام؟ قلت له وأضمن منين أن الحاجات دي متطلعش بعد ما أدفع! قفل السكة في وشي. في نفس اليوم اكتشفت إن واحدة صاحبتي من اللي كانوا معانا يومها حصل معاها نفس الموضوع بالظبط!

لجئنا وقتها لواحد صاحبنا عندهم محل موبايلات كبير أخد موبايلتنا وعمل عليها حاجات مش عارفنها وبعدها سألنا لو كنا بندخل على واي فاي في أماكن عامة فقلنا له آه عادي. قالنا اننا لازم نعمل بلاغ ونتتبع الشخص اللي بيبتزنا، اضطرينا نقول لأهلنا وبلغنا وقدرنا نستدرجه واكتشفنا بعدها انه شخص شغال في الكافيه اللي قعدنا فيه آخر يوم امتحان. من ساعتها أنا وصاحبتي في حالة رعب لأننا مش عارفين لو الصور اللي معاه دي في منها نسخ تانية ولا لأ وممكن يستخدمها للانتقام مننا ولا لأ.











إجراءات الدخول على أى شبكة إنترنت عامة بأمان:

مهم نعرف أن أي شبكة إنترنت في على الأقل شخص مسئول عن إدارتها وصيانتها وهو "مدير الشبكة" أو مسئول نظم المعلومات في المكان وأن الشخص قد يكون لديه كامل التحكم بالاتصال وقادر على العديد من الأمور منها على سبيل المثال منع وحجب بعض المواقع، وتحديد سرعات الاتصال للأشخاص المتصلين بالشبكة، والاطلاع على المواقع التي يستخدمها المتصلين بالشبكة، والتلاعب بالبيانات والمحتوى الذي يحصل عليه المتصلين بالشبكة بكافة الأشكال ويمكنه أيضًا (في حال كانت عنده الخبرة اللازمة) سرقة البيانات الشخصية التي يتداولها المتصلين بالشبكة أثناء اتصالهم في حالة استخدامهم برمجيات غير آمنة ومعمّاة.

استخدام شبكة تور، بروتوكول التوجيه البصلي (TOR)، اللي بيعمّي الاتصال بالإنترنت وبيساعد في إخفاء هويتك وموقعك الحقيقي على الإنترنت، و يحمي أيضًا بياناتك من التلاعب والسرقة، وبيساعد كمان على تجاوز إجراءات الحجب.

ندخل دايمًا على المواقع التي تستخدم بروتوكول نقل النص التشعبي الآمن (HTTPS)، عشان بتُعمّي الاتصال بينك وبين الخدمة أو الموقع اللي بتزوره في الاتجاهين، وبتخلي المتصفح يتحقق من هوية الموقع للتأكد من عدم التوجه لموقع آخر ينتحل هوية الموقع المقصود الدخول عليه، وده بيحميك من الوقوع ضحية لهجمات الانتحال ومن اعتراض بياناتك أثناء اتصالك بالمواقع أو تعديلها والتلاعب بها. وضروري كمان نقرأ رسائل الخطأ بالمتصفح، عشان ممكن تكون تحذير من هجمة ما أو موقع ينتحل هوية الموقع المقصود.

ما تشاركش بيانات حساسة من خلال شبكة عامة، حتى بعد الحرص على تطبيق كافة النصائح السابقة، أو على الأقل التأكد من استخدام وسائل اتصال معمّاة مخصوصة.

الأدوات والبرمجيات المقترح استخدامها في تلك الحالة:

متصفح تور. رغم حجب موقع مشروع تور في مصر يمكن الوصول لمرآة للموقع عن طريق الرابط tor.eff.org.

إضافة ملحقة HTTPS Everywhere لمتصفحك، حتى يمكن ضبطها لإجبار المتصفح على الاتصال بالمواقع فقط من خلال الإصدار الآمن من بروتوكول نقل النص التشعبي (HTTP).

القصة الخامسة

"حساب مزيف كل يوم!"

ما حكيتش القصة دي لحد ومش عارفة ليه، يمكن كنت بحسها تافهة أو مش مهمة أو يمكن كنت عايزة أنساها وأخلص منها أو يمكن بتكسف منها. من حوالي ٦ سنين كنت مخطوبة وخلال فترة خطوبتي ظهر فجأة واحد علي تويتر كان يبدو إنه مهووس بيا شوية بيرد علي أي حاجة بكتبها وبيدخل جوا أي محادثة بيني وبين أي حد تاني، وبعدين مش فاكرة ليه أو إزاي الموضوع اتطور وبدأ يرد ردود فيها مضايقة ليا ولأصدقائي، يمكن كان سألني حاجة أو قال حاجة وأنا رديت رد بايخ وهو أخدها على نفسه...

حقيقي مش عارفة، اللي أعرفه إني فجأة صحيت يوم من النوم على كذا حساب مزيف ليا وكنت كل ما ببلغ في الموقع عن واحد يطلع مكانه خمسة! في الأول كان بيعمل حسابات على تويتر وفيسبوك بشخصيتي، على فيسبوك كان سهل جدا يتمسحوا لأن أول ما ببلغ إدارة فيسبوك سريعة في ده، لكن تويتر الوضع مختلف.

بعد شوية الحسابات دي ابتدت تبقى إباحية، افتكر منهم اكاونت سماه ”فخاد كذا (اسمي بالكامل)“. طبعا خطيبي وقتها كان هينهار وفضل يطلب مني أقفل تويتر وفيسبوك تماما لكن دا ما كانش حل. قفلته أسبوع وأنا مجبرة، وبعدها فتحته عشان حسيت إن مش معقول هآخد قرارات في حياتي على مزاج واحد مريض. ما ماكانتش فاهمة هو عايز إيه لكن كنت كل ما بتجاهله كل ما بيزيد فيها، حاولت أدور على مخترق لأن الموضوع وصل لمراحل فعلا مؤذية لما ابتدى يبعت لأصدقائي ويقول كلام جارح وغير أخلاقي، زي لما بعت يقول لخطيبي ”دي شاذة وبتستخدمك عشان تضحك علي المجتمع“.

اللي بفكر فيه بعد التجربة دي هو إن أنا لو كنت في بيئة أو قرية أو بلد محافظة وده حصل كنت هتجرس ومش بعيد أهلي أو حد من قرايبي يضربني أو يقرر يجوزني بالعافية، ولو كنت متجوزة كان احتمال جوزي طلقني مثلا لأن دا اللي عادة بيحصل هنا، الذنب دايما ذنب البنت.



في حالة وجود حسابات وهمية باسمك:

ضروري إبلاغ أصدقائك ومتابعيك وتحذيرهم إنهم ما يتعاملوش مع الحسابات دي

تطلب من أصدقائك عمل بلاغات لإدارة شبكة التواصل الاجتماعي لتلك الحسابات، وما تكتفيش فقط ببلاغك الشخصي.

القصة السادسة

"أكيد مش هنسى كلمة سر بتاريخ ميلادي!"

أنا شخص ذاكرته ضعيفة جدًا وبنسى كل حاجة بسهولة، من وقت ما دخلت على الإنترنت وأنا تقريبًا عامل كلمة سر واحدة لكل حاجة، فضلت سنين طويلة بستخدم تاريخ ميلادي كلمة سر للإيميل وفيسبوك وحتى موبايلي نفسه واللابتوب، عشان أكيد مش هنسى تاريخ ميلادي! في يوم بفتح الإيميل لقيته بيقولي wrong password، فضلت أجرب أكتر من مرة وأشوف لو كنت مغير لغة الكيبورد أو فاتح ال Caps lock، ما فيش، كل حاجة زي ما هي والإيميل مش عايز يفتح! قلت أفتح فيسبوك لقيته كمان مش بيفتح! قلت أكيد حساباتي كلها اتسرقت! بقيت مش عارف اتصرف!

حاولت بكل الطرق أرجع الحسابات ما عرفتش غير لما واحد صاحبي شاطر في الكمبيوتر شوية ساعدني فقدرنا نرجع الإيميل اللي كنت برضه مش عامل أي خطوات أمان عليه وكذلك فيسبوك.

طبعًا اكتشفت بعدها ان المشكلة كانت في كلمة السر وإن غالبا اللي قرر يخترق الحساب حد عارفني فقدر يتوقع كلمة السر بتاعتي ولأني ما كنتش عامل إجراءات حماية كافية على إيميلي قدر يدخل بسهولة من غير ما جوجل يتأكد إنه أنا، بس طبعًا مقدرناش نعرف هو مين، لحد دلوقتي عندي مشكلة النسيان بس مش عايز تحصلي نفس المشكلة تاني، فدايما بنسى كلمة السر وبفضل أعملها reset كل شوية.



عشان تختار كلمة سر قوية:

تفادي كلمات السر سهلة الاستنتاج عن طريق التخمين أو معرفة بعض المعلومات الشخصية عنك.

عدم استخدام نفس كلمة السر لأكثر من حساب، لان ساعات بيتم تسريب قواعد بيانات شركات ضخمة مثل ياهو وعادة بيستخدم المخترقون قواعد البيانات المسربة في تنفيذ هجوم تخمين كلمة السر.

تفعيل خدمات التأمين اللي بيقدمها معظم مقدمي خدمات البريد الإلكتروني مثل جوجل.

مهم جدًا تغيير كلمات سر الحسابات الشخصية والبيانات الحساسة بشكل منتظم وعلى فترات ثابتة.

استخدام كلمة سر معقدة قدر الإمكان.

ممكن استخدام إحدى برمجيات توليد وتخزين وإدارة كلمات السر العشوائية للقيام بالمهمة دي.

لو عارف إن المواد اللي بتشاركها على بريدك حساسة وممكن تعرضك للخطر، دي خطوات مهمة:

ممكن تستخدم منصات تقدم خدمة البريد الإلكتروني مع تفعيل خاصية تعمية الرسائل بكلمة سر زي ProtonMail و Tutanota

Riseup، منصة مهتمة بتقديم دعم تقني للنشطاء في شتى مجالات العمل العام، بتقدم خدمات زي البريد الإلكتروني واتصال الشبكة الافتراضية الخاصة VPN وخدمات أخرى (آمنة ولا تحتفظ ببيانات عن المستخدمين ورسائلهم لكن مش بتدعم التعمية من الطرف للطرف بشكل افتراضي حتى الآن).

ممكن تستخدم Thunderbird مع Enigmai، برنامج عميل لخدمة البريد الإلكتروني من تطوير شركة موزيلا مع إضافة لتفعيل إرسال واستقبال رسائل البريد الإلكتروني المعماة وإدارة المفاتيح العامة بتقنية GPG.

الأدوات والبرمجيات المقترح استخدامها في تلك الحالة:

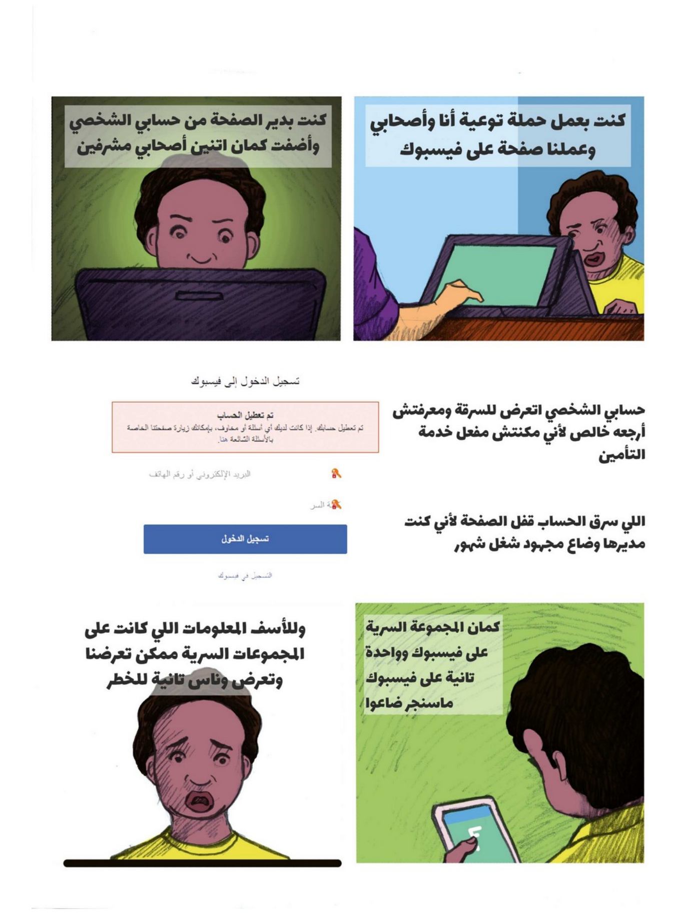
KeePassXC

القصة السابعة

"الحساب والصفحة والمجموعة ضاعوا مرة واحدة!"

كنت بشتغل على حملة توعية من فترة، وقررت أنا ومجموعة من صحابي المهتمين بنفس الموضوع، إننا نعمل صفحة على فيسبوك عشان نقدر ننشر من عليها فعاليات الحملة وأي محتوى بنقدمه للجمهور المستهدف. بالفعل عملت الصفحة من حسابي الشخصي وضفت ٣ أصدقاء تانيين يكونوا مراقبين للصفحة معايا عشان نقدر ننسق مع بعض النشر وإضافة المحتوى والرد على الرسايل.

بعد فترة اتعرضت لسرقة حسابي اللي كنت عامل بيه الصفحة، وللأسف مقدرتش أرجعه، ولأني ماكنتش مفعل خدمة التأمين على فيسبوك، واللي سرق الحساب قفل الصفحة ومقدرناش نرجعها لأن انا كنت المدير و منشئ الصفحة وضاع مجهود شهور شغل على الصفحة، غير كده إننا كنا عاملين مجموعة سرية على فيسبوك ومجموعة تانية على فيسبوك ماسنجر، وأنا اللي كنت عاملهم برضه، عشان ننسق عليه الشغل مع بعض بسهولة، وطبعًا المجموعة كمان ضاعت زي الصفحة، وكان عليها شغل ومعلومات تعرضنا وتعرض ناس تانية كمان للخطر.



لحماية مجهودك و شغلك على صفحة فيسبوك:

تفيعل خاصية الاستيثاق بمعاملين (Two Factor Authentication).

استخدام حساب مجهول لإدارة الصفحة.

الاعتماد على مديرين آخرين للصفحة، أيضًا بحسابات حقيقية.

الابتعاد عن استخدام فيسبوك ماسنجر لإرسال رسائل لأعضاء مجموعة الفيسبوك القائمة على إدارة الحملة.

عدم استخدام منصات غير معماة وغير موثوقة في إرسال الصور والبيانات.

الابتعاد عن مشاركة البيانات على مجموعة سرية على فيسبوك (في حالة إنشاء مجموعة سرية من المهم أن يكون المستخدم على دراية أن سرقة أي حساب من حسابات أعضاء المجموعة قد يعرض باقي المجموعة للخطر، لأنه يسهل للمخترق الوصول إلى كل البيانات المتاحة لأعضاء المجموعة).

في حالة ضرورة استخدام فيسبوك للتواصل ومشاركة البيانات في مجموعة سرية، ننصح باتباع الآتي:

التخلص المستمر من البيانات والمعلومات الحساسة.

عدم مشاركة بيانات ومعلومات حساسة أو شخصية من خلال منصة غير معمّاة أو غير موثوقة.

عدم الاحتفاظ بجلسات تسجيل الدخول على الأجهزة المستخدمة طوال الوقت.

عمل حسابات مجهولة لإدارة الصفحة، وإنشاؤها من خلال اتصال بشبكة تور، وعدم استخدام أي رقم هاتف لأي عضو في مجموعة العمل لأن ممكن يعرضهم للخطر، في حالة وجود بيانات حساسة.

تفعيل الاستيثاق بمعاملين (two factor authentication)، لأي حسابات شخصية.

استخدام منصات تواصل لحظي معمّاة ومفتوحة المصدر تحترم المستخدم وتولي أهمية لسرية بياناته.

الوعي باتفاقية حقوق المستخدم في فيسبوك، وطبيعة الموقع عامة فيما يخص سياسة الخصوصية وحماية البيانات.

الأدوات والبرمجيات المقترح استخدامها في تلك الحالة

Tor Browser

https://facebookcorewwwi.onion

.Google Authenticator

Signal Private Messenger

Wire Private Messenger

الدليل التقني لاستخدام الأدوات والتطبيقات

أولًا التعمية

التعمية (Encryption) هي عملية تحويل البيانات من شكلها المقروء أو الواضح إلى شكل لا يمكن قراءته أو معاينته إلا للمخولين بذلك. ويمكننا تعمية البيانات بعدة طرق:

تعمية قرص نظام التشغيل

تدعم أنظمة التشغيل إمكانية تعمية البيانات الموجودة على وحدة التخزين، بحيث لا يمكن الوصول إلى هذه المعلومات إلا بعد الإقلاع من نظام التشغيل وتسجيل الدخول بنجاح إلى حساب المستخدم. بعد تسجيل الدخول يتيح نظام التشغيل المعلومات الموجودة على القرص للمستخدم عند الحاجة لها، مبقيا عليها معماة على القرص. يذكر أيضا أن أنظمة تشغيل الهواتف الذكية سواء كانت iOS أو أندرويد تدعم أيضا هذه الإمكانية.
التعمية الكاملة أو الجزئية للقرص الصلب علي أنظمة تشغيل جنو/لينكس

تدعم أغلب أنظمة التشغيل الشبيهة بيونكس والتوزيعات المبنية عليها تعمية القرص الصلب كليًا أو جزئيًا أثناء تهيئته أثناء التنصيب، ولكن نظرًا لتعدد تلك الأنظمة يصعب حصر الطريقة في عدة خطوات واضحة.

إذا كنت مستخدم حالي لأنظمة شبيهة بيونكس ولك بعض الخبرة في التعامل معها، فأنت في الغالب تعلم بالفعل كيفية تعمية القرص الصلب عن طريق LUKS سواء بعد عملية التنصيب أو خلالها.

إذا كنت من مستخدمي شبيهات يونكس (جنو/لينكس، BSD) ولا تعلم كيفية تفعيل تعمية القرص الصلب فمن الأفضل استشارة متخصص قبل التجربة لأول مرة.

إذا كنت تخطط للانتقال لاستخدام أحد الأنظمة الشبيهة بيونكس بشكل أساسي يفضل مراجعة الأدلة التقنية الخاصة بالتوزيعة التي اخترت استخدامها قبل بداية التنصيب لمعرفة كيفية تفعيل تعمية القرص الصلب أثناء التنصيب.

تنبيه: تفعيل التعمية الكاملة أو الجزئية للقرص الصلب على الأنظمة الشبيهة بيونكس يستدعي بالضرورة إعادة تهيئة كامل القرص الصلب، وسوف ينتج عن ذلك فقدان جميع البيانات المخزنة عليه، لذلك ننصحك بضرورة عمل نسخة احتياطية من البيانات قبل التعمية.
تعمية قرص نظام التشغيل على ويندوز

يدعم نظام التشغيل ويندوز بنسخــه الاحترافية، سواء ويندوز برو (Windows Pro) أو ويندوز للشركات (Windows Enterprise)، تعمية القرص الصلب باستخدام التطبيق BitLocker الذي يأتي مدمجا مع نظام التشغيل.

تنبيه: مع تشغيل BitLocker للمرة الأولى تأكد من توليد رمز استرداد القرص المعمى وحفظه في مكان آمن، لكي تستخدمه في حال خسرت كلمة سر نظام التشغيل أو في حال تلف نظام التشغيل لسبب ما واحتجت لنقل معلوماتك من القرص إلى مكان آخر.

لتفعيل الميزة اتبع الخطوات التالية:

1- من خانة البحث في نظام التشغيل Windows 8 أو Windows 10 ابحث عن BitLocker ثم الضغط على بحث

2- اضغط على تشغيل BitLocker لتفعيل الميزة. لكي تستطيع ذلك يجب أن يكون لديك صلاحيات المدير. وقد يقوم نظام التشغيل بطلب إدخال كلمة سرّ مدير النظام.

3- يبدأ تطبيق BitLocker بالعمل، اتبع التعليمات التي تظهر على الشاشة لإتمام العملية للمرة الأولى.

بعد الانتهاء يصبح القرص الصلب الذي يحتوي نظام التشغيل معمّى ويزول خطر تعرض البيانات للوصول ليد سارق الحاسب في حال سرقته.

للاطلاع على خطوات مفصلة ومدعومة بصور توضيحية يمكنك زيارة الرابط pcworld.com/article/2308725/encryption/a-beginners-guide-to-bitlocker-windows-built-in-encryption-tool.html

تعمية قرص نظام التشغيل على ماك أو إس (macOS)

يقدم نظام التشغيل ماك أو إس، ابتداء من إصدارة OS X Lion فصاعدا، إمكانية تعمية القرص الصلب الذي يحتوي نظام التشغيل عليه عبر تطبيق FileVault الذي يأتي جزءً من نظام التشغيل. تطبيق FileVault يستخدم تعمية XTS-AES 128. لتفعيل ميزة تعمية القرص الصلب اتبع الخطوات التالية:

1- تأكد من وصل الجهاز إن كان محمولا إلى الشاحن.

2- افتح FileVault من إعدادات الأمان والخصوصية Security & Privacy ضمن واجهة إعدادات النظام System Preferences.

3- اضغط على رمز القفل وادخل كلمة السرّ الخاصة بك لكي تتمكن من تعديل الإعدادات المرتبطة بـ FileVault.

4- اضغط على Turn On FileVault.

5- إذا كان لديك عدد من المستخدمين على جهاز ماك. يمكنك إعطائهم صلاحية تشغيل الجهاز. إن لم تفعل يمكنهم دخول حساباتهم بعد أن يقوم الأدمن بالإقلاع. لإعطاء الصلاحية اضغط على Enable User وأدخل كلمة سرّ المستخدم (أو دعه يضع كلمته الخاصة)واضغط على Ok.

6- بعد أن تمت عملية إعداد FileVault أعِد تشغيل الجهاز عبر الضغط على Restart.

7- ستظهر الواجهة التالية طالبة كلمة السرّ.

8- يبدأ التطبيق بتعمية القرص للمرة الأولى. ستأخذ هذه العملية بعض الوقت لكنها ستجري في الخلفية متيحة لك استخدام الجهاز كالعادة. أي ملفات جديدة تنشئها خلال هذه العملية وفي المستقبل ستكون معمّاة تلقائيا. ستتوقف عملية التعمية للمرة الأولى عند انتهاء التعمية, أو عند إطفاء الجهاز لتتابع فيما بعد.

تنبيه: يجب إعداد خيارات استرجاع القرص، أي إعداد الخيارات الاحتياطية لفك تعمية القرص عن طريق الخطوات التالية:

1- يمكنك حفظ رمز لإستعادة القرص على حساب iCloud.

2- يمكنك أيضا حفظ الرمز مع عدد من الأسئلة والأجوبة تحتفظ بها شركة Apple التي تخولك استعادة الرمز بالاتصال بشركة أبل والإجابة عن الأسئلة.

3- يمكنك طلب الرمز مباشرة خلال إعداد التعمية، قم بحفظ هذا الرمز في مكان آمن (بالتأكيد ليس على الجهاز نفسه) اضغط على رمز المثلث لكي يظهر الرمز إن كان مخفيا.

للاطلاع على خطوات مفصلة ومدعومة بصور توضيحية يمكنك زيارة support.apple.com/en-us/HT204837

تعمية جهاز آيفون (iPhone)

بالنسبة للأجهزة العاملة بنظام التشغيل iOS مثل آيفون iPhone وآيباد iPad فالأمر بغاية البساطة، فبمجرد وضع كلمة سرّ أو رمز PIN للجهاز تفعّل ميزة تعمية الجهاز. بدون كلمة السرّ أو الرمز لا يمكن فك التعمية. إن كان للجهاز كلمة سرّ أو رمز PIN فالجهاز معمى بالفعل. أما إن لم يكن هناك كلمة سرّ أو رمز لقفل الشاشة فيتوجب وضعها عبر اتباع الخطوات التالية:

1- توجه إلى الإعدادات Settings.

2- اختر Touch ID & Passcode.

3- اختر تشغيل رمز المرور Turn Passcode On وضع كلمة سرّ جيدة لجهازك.

تعمية جهاز أندرويد

يتيح نظام التشغيل أندرويد إمكانية تشغيل الأجهزة العاملة بنظام أندرويد سواء كانت هواتف ذكية أوحواسب لوحية. لتفعيل ميزة التعمية على هذه الأجهزة اتبع الخطوات التالية:

1- توجه إلى قائمة الإعدادات Settings ثم إلى قسم الأمان Security

2- إن كنت تستخدم كلمة سرّ لحماية هاتفك تابع إلى الخطوة التالية. أما إن كنت لا تستخدم قفل للشاشة أو إن كنت تعتمد على طرق أخرى لقفل الشاشة، فعليك تعديل قفل الشاشة بوضع كلمة سرّ لحماية الجهاز. اختر قفل الشاشة Screen Lock، وضع كلمة سرّ مناسبة لحماية جهازك.

3- تأكد من أن الجهاز متصل بالشاحن وأن البطارية مشحونة لمستوى ٨٠٪.

4- اختر تعمية الجهاز Encrypt Phone.

5- انتظر اكتمال عملية التعمية.

يتيح أندرويد أيضا إمكانية تعمية بطاقة الذاكرة SD Card. ويمكن تفعيلها عبر اتباع الخطوات التالية:

1- توجه إلى قائمة الإعدادات Settings ثم إلى قسم الأمان Security.

2- اختر تعمية قرص SD وتابع الخطوات.

لاحظ أن مع تعمية القرص SD لن تتمكن من استخدام البيانات الموجودة عليه إلا على جهاز أندرويد نفسه، ويجب إعادة تهيئته في حال رغبت باستخدامه على جهاز جديد (طبعا بدون البيانات التي كانت موجودة عليه).

تعمية الأقراص والملفات

توجد برامج تعمية للأقراص الصلبة والملفات، و هي برامج مصممة لحماية المعلومات الموجودة على الأقراص عبر تقنية تجعل المعلومات المخزنة على القرص معمّاة. تظهر هذه البرامج محتوى الملفات المعمّاة الموجودة على القرص المعمّى عبر فك تعميتها عندما يطلبها مستخدم معه كلمة

السر الصحيحة التي استخدمت لحماية المعلومات المعمّاة. برامج تعمية الأقراص يمكن أن تستخدم لإخفاء بيانات ضمن القرص المعمّى بحيث يستطيع صاحب البيانات إخفاء حقيقة وجودها في حين لا يمكن لأحد إثبات وجود هذه المعلومات في ما يسمى الإنكار القابل للتصديق (Plausible Deniability).

أحد أكثر برامج تعمية الأقراص التي لها هذه الخاصية هو برنامج فيراكريبت (VeraCrypt)، وهو برنامج تعمية أقراص يعمل على أنظمة تشغيل متعددة سهل الاستخدام وله سمعة طيبة. ويعطي مستخدمه إمكانية تعمية المجلدات وأيضا تعمية الأقراص الصلبة والمحمولة. بالإضافة لذلك، يوفر أيضا امكانية الإنكار القابل للتصديق Plausible Deniability عبر المجلدات المخفية ضمن القرص المعمّى.

للاطلاع على خطوات تنصيب فيراكريبت للمبتدئين مدعومة بصور توضيحية يمكنك زيارة veracrypt.fr/en/Beginner's

Tutorial.html

ثانيًا: خدمات التخزين السحابي للبيانات

توجد اليوم المئات من المواقع التي تقدم خدمة التخزين السحابي (Cloud Storage)، ولكن لا يمكننا الوثوق بجميعها، حيث أن العدد الأكبر من هذه الخدمات هدفه تجاري بالأساس، وذلك يجعل الباب مفتوحا أمام احتمال بيعهم لهذه البيانات المخزنة أو تسليمها إلى الحكومات أو السلطات في حال طالبت بها.

لذا في البداية قبل اختيار الخدمة التي نريد استخدامها لتخزين نسخنا الاحتياطية، من المهم أن نتأكد من التالي:

1- قراءة اتفاقية الخصوصية وشروط الاستخدام التي تنشرها جميع هذه المواقع للتأكد من أن بياناتنا في أمان.

2- يجب أن تدعم الخدمة ميزة نقل البيانات الآمن عبر بروتوكول HTTPS وذلك للتأكد من أن نقل البيانات بين حاسوبك وخدّمات هذا الموقع لا يستطيع المخترقين أو مزود الخدمة أو الحكومات اعتراضها.

3- التحقق من أن هذه المواقع تتيح خيار تعمية البيانات.

في حالة الاستخدام الشخصي، نرشح خدمة ميجا للتخزين السحابي، إذ تتوفر في ميجا مميزات الخصوصية والأمان المذكورة أعلاه، والتي بالمناسبة لا توفرها خدمة التخزين السحابي الشهير دروب بوكس مثلا.

يتيح ميجا، تعمية البيانات على الخادوم، مما يعني أنه لا يمكن لأحد الوصول إلى بياناتك، حتى أصحاب الموقع ذاتهم.

ومن أهم مميزاته الآتي:

1-يتيح ميجا خدمات التخزين السحابي من خلال المتصفح وأيضًا من خلال برنامج يمكنك تنصيبه على جهازك الشخصي، ويتميز ميجا أنه يتيح برامجه لكل أنظمة التشغيل (لينكس، ويندوز وماك).

2- يمكنك أيضًا تنصيب برنامج ميجا للتخزين السحابي، على هواتف أندرويد، آبل وحتى ويندوز من خلال تنصيبه من متجر البرامج.

3- يمكنك إتاحة خدمة التخزين الأوتوماتيكي لبيانات هاتفك مباشرةً على ميجا، بدل من تخزينه على خدمات أقل أمانًا مثل جوجل درايف.

4- يتيح ميجا من خلال برمجيات الحواسيب أو الهواتف وحتى من خلال موقعه، خدمة التراسل اللحظي Megachat، والتي تعتبر خدمة آمنة لأنها تعتمد على بروتوكول التعمية من الطرفين (End to end encryption)، وذلك للرسائل المكتوبة والصوتية والمكالمات أيضًا.

يمكنك تحميل تطبيق ميجا مباشرة من خلال الرابط mega.nz/startpage

ثالثًا: مشاركة الملفات مع آخرين بشكل معمى

في حال رغبت في مشاركة ملفات بشكل معمى مع آخرين بطريقة سهلة، يمكنك استخدام خدمة فَيَرفُكس سيند، التي أطلقتها موزيلا في أغسطس ٢٠١٧، ومن أهم مميزاتها:

1- تسمح لك برفع ملفات يصل حجمها إلى ١ جيجا بايت وتعميها.

2- توفر لك رابط للملف المرفوع، قابل للمشاركة مع أي شخص ومن خلال أي وسيلة تواصل رقمية.

3- تمسح الملف المعمّى من خادوم فَيَرفُكس سيند بعد ٢٤ ساعة من رفعه عليه أو بعد تنزيله مرة واحدة من أي شخص شاركت معه الرابط معه.

4- يمكنك استخدام فَيَرفُكس سيند من أي متصفح، دون الحاجة لإضافة ملحقات له.

للاطلاع على كيفية استخدام خدمة فَيَرفُكس سيند يمكنك مشاهدة الفيديو التوضيحي youtu.be/ZGWZGYtAS3U، ويمكنك زيارة موقع الخدمة في send.firefox.com.

رابعًا: خدمات المراسلات الآمنة وتعمية الرسائل

البريد الإلكتروني

بداية، في هذه الجزئية الخاصة بالمراسلات عبر البريد الإلكتروني، علينا معرفة الفرق بين مزود خدمة البريد الإلكتروني وتطبيق إدارة البريد الإلكتروني. مزود خدمة البريد الإلكتروني مثل جيميل وياهو وهوتميل، أما تطبيقات إدارة البريد الإلكتروني مثل مايكروسوفت أوت لوك، ثندربيرد وأوبرا ميل.

نعرف أن الكثير منا الآن يفضل استخدام مزود خدمة البريد الإلكتروني الخاص بجوجل، ولكن في حالة إذا كانت رسائلك حساسة وقد تعرضك أنت وآخرين للخطر، ننصحك باستخدام مزود خدمة البريد الإلكتروني توتانوتا.

توتانوتا، هو مزود خدمة بريد إلكتروني مفتوح المصدر، يقوم بالأساس على مبدأ تعمية رسائلك بشكل تلقائي، يتضمن ذلك محتوى الرسالة، عناوين المتصلين، المرفقات وعنوان الرسالة. يتميز توتانوتا بالآتي:

1- يمكنك تعمية رسائلك الإلكتروني مع الأفراد الذي ترغب التواصل معهم حتى إذا كانوا مستخدمين لمزودات خدمات بريد إلكتروني أخرى مثل جوجل او ياهو أو غيرهم عبر استخدام خاصية كلمة سر التعمية.

2- يستخدم توتانوتا خاصية التعمية من الطرف إلى الطرف End to End Encryption.

3- يتيح لك توتانوتا خصية GPG، ولكن يجب أن يكون للطرفين مفاتيح لتعمية رسائلهم.

4- في حالة إرسال رسالة لاكثر من شخص من مستخدمي المزودات الأخرى، يتيح لك توتانوتا خاصية كلمة سر لتعمية الرسالة لكل فرد منهم بشكل منفرد.

5- يوفر لك توتانوتا تطبيقات آمنة على هاتفك المحمول اذا كان أندرويد أو iOS، ويمكنك تنصيبه عبر متجر التطبيقات.

ملاحظات هامة في حالة استخدام توتانوتا:

1 -لا ينصح بفتح مزود البريد الإلكتروني، توتانوتا، إلا من أجهزة تتوفر فيها عوامل الأمان اللازمة مثل أنظمة تشغيل آمنة وتعمية القرص الصلب.

2- ينصح بفتح بريدك الإلكتروني على توتانوتا من متصفح آمن مثل فَيَرفُكس أو تور.

3-في حالة إذا كانت التعمية جريمة في بلدك، ننصحك بعدم استخدام بريدك على توتانوتا، بشكل دائم حتى لا يلفت ذلك انتباه السلطات لك.

للاطلاع على كيفية التسجيل وإرسال الرسائل الإلكترونية على توتانوتا، يمكنك مشاهدة هذا الفيديو التوضيحي youtu.be/qUgQxxhr3EY، ويمكنك إنشاء حسابات على توتانوتا من الرابط app.tutanota.com/#register.

بعد الحديث عن مزودات خدمات البريد الإلكتروني، والحديث عن المزود الذي ننصح به وهو توتانوتا، يأتي الآن الحديث عن برمجيات إدارة البريد الإلكتروني، فإذا كان لديك بريد إلكتروني على أكثر من مزود خدمة وتريد إدارة رسائلك عبر منصة واحدة فقط، نرشح لك برنامج ثندربيرد، هو برنامج حر ومفتوح المصدر، يتيح لك تبادل وحفظ رسائل البريد الإلكتروني لعدّة حسابات ومن عدة مزودات خدمة. من أهم مميزات ثندربيرد الآتي:

1- يتيح لك ثندربيرد إضافة كافة عناوينك عبر مزودات خدمة بريد إلكتروني مختلفة، مما يسهل عليك تجميع رسائلك في منصة واحدة فقط.

2- إمكانية قراءة وتحرير الرسائل دون اتصالٍ بالإنترنت.

3- إمكانية إرسال واستقبال الرسائل الإلكترونية المُعمّاة.

4- يتميز ثندربيرد بواجه خارجية تشبه واجهة متصفح فَيَرفُكس، فيمكنك من خلالها فتح أكثر من رسالة إلكترونية في عدة تبويبات.

5- تستطيع من داخل ثندربيرد أن تتصفح الوب، عبر استخدام زر البحث أو من خلال اختيار كلمات محددة في رسائلك واختيار خاصية البحث على الوب.

6- يتيح لك ثندربيرد خاصية ترشيح لرسائلك، بمعنى أنه يمكنك اختيار كلمات أو موضوعات محددة، فيستطيع هو تحديد الرسائل التي تشمل تلك الكلمات والموضوعات بسهولة.

7- تستطيع من داخل ثندربيرد نفســـه، إضــافة أي امتــدادات (Extensions).

8- تستطيع عمل مجلدات داخلية على ثندربيرد، لإدارة رسائلك.

9- يتمتع ثندربيرد بميزة هامة، انه يحميك من حملات الاحتيال، وهي إحدى طرق اختراق الإلكتروني الشهيرة.

10- يعمل ثندربيرد على كافة أنظمة التشغيل على الحواسيب مثل لينكس، ويندوز وماك.

إذا اخترت ثندربيرد لإدارة رسائلك الإلكترونية، فذلك سيعطيك ميزة إضافية للتمتع بخصوصية وأمان أكبر لأنك تستطيع إضافة إنجميل (Enigmail)، وهي إضافة لثندربرد تُمكّنك من الوصول لمزايا التعمية والاستيثــاق التي يتيحهــا حــارس خصوصيــة جنو (GnuPG)، والذي يجب أن يُثبّت ليعمل إنجميل.

للاطلاع على كيفية إدارة الرسائل الإلكترونية على ثندربيرد وطرق تنصيب إنجميل لتعمية رسائلك، يمكنك تتبع الخطوات التفصيلية على هذه الروابط، لمستخدمي لينكس: securityinabox.org/ar/guide/thunderbird/linux ولمستخدمي ويندوز: securityinabox.org/ar/guide/thunderbird/windows.

التراسل اللحظي الآمن

يعتمد أغلبنا على خدمات تراسل لحظي شائعة دون التأكد من توافر عوامل الأمان الأساسية بها، على سبيل المثال لا يمكن التعامل مع خدمة التواصل اللحظي في فيسبوك على أنها خدمة آمنة حيث لا توجد أي تأكيدات حقيقية على مستويات التعمية المستخدمة بها.

يجب أن يوضع في الاعتبار أيضًا أن استخدام أغلب خدمات التواصل اللحظي عمومًا، والخدمات المضمنة في منصات التواصل الاجتماعي خصوصا، يعني أن البيانات والرسائل التي تشاركها يحتفظ بها بشكل أساسي في ثلاثة أماكن (حساب المرسِل، خواديم المنصة، حساب المستقبِل)، وهذا يوضح أن حذف المحتوى أو الرسالة من طرف واحد لا يعني أنها تم التخلص منها، حيث أنها ما زالت موجودة في أماكن أخرى.

لذلك من الأفضل عند الرغبة في إرسال بيانات شخصية حساسة (يخشى عند فقدانها أو الاستيلاء عليها تعرض صاحبها للخطر)، استخدام منصات وبرمجيات أخرى مثل Signal و Wire، وهي برمجيات مفتوحة المصدر التي تعمِّي المحتوى من طرف المستخدم ولا تحتفظ بالبيانات في صورة غير معمّاة. يتمتع هذان البرنامجان بنفس الخصائص الموجودة على البرمجيات الأخرى التي لا يتوفر فيها عوامل الأمان فيمكنك مشاركة الرسائل النصية والصوتية وعمل مكالمات هاتفية بالإضافة لمشاركة الصور والفيديو وحتى استخدام الإيموجي.

يمكنك تحميل Signal و Wire من خلال متجر التطبيقات على هواتفك المحمولة أيًا كان نظام تشغيلها أندرويد أو iOS.

خامسًا: المتصفحات الآمنة والملحقات الضرورية

فَيَرفُكس

نعلم جميعًا ضرورة وأهمية المتصفحات في تعاملنا اليومي مع الإنترنت، وبالرغم من استخدام أغلبنا أيضًا للمتصفح الأكثر شيوعًا حاليا وهو جوجل كروم، إلا أننا ننصح بشدة استبداله بمتصفح موزيلا فَيَرفُكس كوانتم.

لماذا موزيلا فَيَرفُكس؟

1- يمنع فَيَرفُكس المتعقبات على الشبكة وأنت تتصفحها ولا يتذكر التاريخ بعد أن تنتهي.

2- بعض الإعلانات متعقبات مخفية تمشي وراءك وأنت تتصفح، ولهذا ابتكر مصممو كوانتم أداة قوية توقفها.

3- بحجب بعض الإعلانات والسكربتات التي تبطئ التصفح، باتت الصفحات تُحمّل أسرع بنسبة ٤٤٪.

4- يُحمّل الصفحات أسرع وأفضل ويستخدم ذاكرة أقل.

يوفّر فَيَرفُكس العديد من الإضافات (add-ons) سهلة الاستخدام، والتي تعمل على تحسين خصوصية وأمان تصفحك للإنترنت. يمكنك اختيار الإضافات التي ترغب بتنصيبها، وضبطها وفقًا لما يناسبك. إذا كنتَ تستخدم حاسوبًا يديره غيرك (في مقهى إنترنت أو في مقر عملك على سبيل المثال) فقد تضطر لإعادة ضبط الإضافات بشكلٍ متكرّر.

ننصح باستخدام إضافة Https Everywhere على أي متصفح، لإجباره على استخدام بروتوكول HTTPS وبالتالي تعمية البيانات المتبادلة بين المتصفح وخواديم المواقع، ما يقطع الطريق على أي طرف ثالث، يسعى إلى معرفة ماهية هذه البيانات المتبادلة. وأيضا لتخفيف احتمال الوقوع ضحية اصطياد كلمات السرّ (Passwords Phishing).

يمكنك تحميل فَيَرفُكس من الرابط mozilla.org/ar/firefox، ويمكنك أيضًا البحث عن الإضافات الهامة لمتصفحك من الرابط addons.mozilla.org/en-US/firefox

متصفح تور

مثلما شرحنا حلولا لتعمية الرسائل الإلكترونية في حال وجود معلومات وبيانات حساسة قد تعرضك لخطر أنت أو الآخرين، ننصح في حالة وجود أنشطة على الوب قد تعرضك لأي خطر أن تستخدم متصفح تور أو بروتوكول التوجيه البصلي، وهو متصفح حر مفتوح المصدر، يعمل على تعمية الاتصال بالإنترنت ويمرر البيانات المعمّاة عبر العديد من نقاط الاتصال مما يساعد في إخفاء هويتك ومكانك الجغرافي وأنت تتصفح الإنترنت، و يحمي أيضًا بياناتك من التلاعب والسرقة، كما يساعد على تجاوز إجراءات الحجب.

يتميز تور بعدة خصائص هامة وهي:

1- يمنع المواقع أو مزودي خدمة الإنترنت من تعقب عادات تصفحك على الإنترنت.

2- يمكن استخدام شبكة تور لنشر مواقع لا يمكن تعقب مكانها.

3- يستخدم تور لاخفاء الهوية عند الدخول في غرف المحادثة أو المنتديات.

4- يحمي تور المستخدمين من مخاطر ما يسمى تحليل حركة البيانات.

يمكنك تحميل متصفح تور على أجهزتك أيًا كان نظام التشغيل المستخدم من الرابط tor.eff.org.

سادسًا: برمجيات توليد وإدارة كلمات السر

إذا كنت من الأشخاص سريعي النسيان، ولديك حسابات على برمجيات ومنصات إلكترونية عديدة، فمن الأفضل استخدام إحدى برمجيات توليد وإدارة كلمات السر، حتى يسهل عليك الأمر، ويجنبك مخاطر اختيار كلمات سر موحدة لكل البرمجيات والمنصات.

ننصح باستخدام برنامج كي باس إكس (KeePassXC)، وهو برنامج حر مفتوح المصدر، وهو عبارة عن خزانة كلمات سر: أي برنامج يمكنك استخدامه من أجل تخزين كل كلمات السر الخاصة بك لكل المواقع والخدمات. خزانات كلمات السر تسمح بتنظيم كل كلمات السر في مكان واحد. خزانة كلمة السر أداة قوية لأنها تسمح باستخدام كلمات سر مختلفة يصعب تخمينها لكل الخدمات بدون الحاجة لتذكرهم، وبدلا من ذلك أنت تحتاج فقط إلي تذكر كلمة السر الرئيسية التي تسمح لك بفتح قاعدة بيانات كلمات السر.

من أهم مميزات كي باس إكس سي الآتي:

1- تخزين أكثر من مجرد أسماء المستخدمين وكلمات السر. فعلى سبيل المثال، يمكنك إنشاء مدخلات لتخزين أشياء هامة مثل أرقام الحسابات أو أرقام منتج أو أرقام متسلسلة أو أي شيء.

2- يمكنك إعداد قفل تلقائي في كي باس إكس ليعمل بعد مرور وقت من انعدام النشاط، فهذا قد يمنع شخص آخر من النفاذ إلي كلمات السر إذا ذهبت بعيدا عن الحاسوب.

3- يمكنك من خلال كي باس إكس تنظيم كلمات السر إلي "مجموعات" في شكل مجلدات.

للاطلاع على كيفية استخدام كي باس إكس يمكنك مشاهدة هذا الفيديو التوضيحي youtu.be/z-cKvTUUgNQ، لتحميل كي باس إكس يمكنك زيارة هذا الرابط keepassx.org/downloads.

سابعًا: الاستيثاق بمعاملين

على الرغم من أهمية اختيار كلمات سر قوية ومعقدة لا يزال من الممكن إختراق بعض الحسابات بأساليب مختلفة مثل هجمات الاحتيال، ولذلك يعتبر الاستيثاق بمعاملين (two factor authentication) حائط دفاعي إضافي أمام تلك النوعية من الهجمات.

الاستيثاق بمعاملين، هو بروتوكول تأمين تبنته أغلب المنصات الشهيرة مثل جوجل و فيسبوك لتأمين حسابات المستخدمين ويعني باختصار أن يعتمد الولوج إلى حساب المستخدم على خطوة إضافية، للتأكد من هويته بعد إدخال اسم المستخدم وكلمة السر، وفي أغلب الأحيان تكون تلك الخطوة هي إدخال سلسلة من أرقام مولدة عشوائيًا وتتغير بعد وقت معين وذلك عن طريق ربط الحساب بتطبيق مخصص لتلك العملية.

يعتبر تطبيق Google Authenticator من أشهر التطبيقات الداعمة لعملية الاستيثاق بمعاملين، ومن أهم مميزاته ما يلي:

1-يمكن استخدامه مع أغلب المنصات الداعمة للبروتوكول وليس فقط تطبيقات جوجل.

2- يمكن تحميل التطبيق مجانًا من متجر التطبيقات الخاص بهاتفك المحمول حيث يتوفر لأنظمة Android و iOS.

يمكن تفعيل البروتوكول على المنصات الداعمة له من داخل إعدادات الأمان الخاصة بكل منصة، لتفعيل التطبيق على منصة جوجل على سبيل المثال اتبع الخطوات على الرابط support.google.com/accounts/answer/1066447.

الخاتمة

حاولنا جاهدين ان نقدم دليلًا تقنيًا سهلًا وبسيطًا، يتناسب مع المستخدم العادي للإنترنت، وإيمانًا منا بأهمية دورنا في رفع الوعي الخاص بالأمان الرقمي للجميع، نرحب دومًا بالأسئلة والاستفسارات عبر كافة وسائل التواصل المتاحة لنا. يمكنكم أيضًا طلب الدعم التقني من متون دومًا، من خلال خدمة العيادة التقنية (عيادة تك)، فقط عليكم ملء هذه الاستمارة https://goo.gl/6X2yYn.